Journal of Algebra **212,** 428–459 (1999)
Article ID jabr.1998.7642, available online at http://www.idealibrary.com on IDEAL®

Isogenies of Polynomial Formal Groups

Robert Underwood*

Department of Mathematics, Auburn University Montgomery, Montgomery, Alabama 36117

Received March 18, 1998

Let $H = H_v(i, j)$ be a Greither order in KC_{p^2} and let Spec $H_v(i, j) \to$ Spec $B \to$ Spec C be a resolution of Spec $H_v(i, j)$ in the flat topology which appears as $\mu_{p^2} \to G_m \times G_m \to G_m \times G_m$ over the field K. Under certain conditions, the formal completions of B and C give rise to two-dimensional polynomial formal groups $\mathscr{F}$ and $\mathscr{G}$, respectively. The given resolution will then translate to an isogeny of polynomial formal groups $\Psi: \mathscr{F} \to \mathscr{G}$ with kernel Spec $H_v(i, j)$.

INTRODUCTION

Suppose K is a finite extension of the p-adic rationals $\mathbf{Q}_p$ with ring of integers R, endowed with the p-adic valuation ν. Let π be a fixed parameter for R with $\nu(\pi) = 1$, and let e be the ramification index of p in R. Assume K contains a primitive p^nth root of unity, denoted ζ_n. Let C_{p^n} denote the cyclic group of order p^n, $\langle g \rangle = C_{p^n}$, and let H be an R-Hopf algebra order in KC_{p^n}, with associated group scheme Spec $H =$ Hom$_{R-\text{alg}}(H, \ )$. By the Oort embedding theorem, Spec H is identified with the kernel of some isogeny Ψ of n-dimensional formal groups $\mathscr{F}$ and $\mathscr{G}$ [3, pp. 3–5]. In this paper we investigate the following question: For which R-Hopf orders in KC_{p^n}, $n = 1, 2$, is Spec H the kernel of an isogeny of *polynomial* formal groups? For $n = 1$ it is known that every R-Hopf order in KC_p represents the kernel of an isogeny of polynomial formal

* The author is indebted to the referee for numerous comments and suggestions which improved this paper considerably.

0021-8693/99 $30.00

groups, see [1, Corollary 1.6]. For $n = 2$, however, it is not clear which R-Hopf orders in KC_{p^2} satisfy this *representability criterion*. We remark that Childs *et al.* have found a class of Hopf orders in $K[C_p \times C_p]$ which represents the kernels of isogenies of polynomial formal groups [2, Theorem 4.3]. In this paper we construct a class of R-Hopf orders in KC_{p^2} which satisfy this representability criterion. Our main result is the following.

MAIN THEOREM (Theorem 5.0). *Let $H = H_v(i, j)$ be a Greither order in KC_{p^2} with $i + j \le e/[p(p-1)]$, $pj \le i$, and $v(1-v) \ge i' + (j/2)$, with $i' = e/(p-1) - i$. Then $H_v(i, j)$ represents the kernel of an isogeny of polynomial formal groups.*

(For the convenience of the reader, we review details on Greither orders here in Section 2.)

We intend to prove the Main Theorem as follows. From [15], we know that there exists a flat short exact sequence of group schemes Spec $H_v(i, j) \to$ Spec $B \xrightarrow{\Theta}$ Spec C where B, C are certain Hopf algebras, which we compute explicitly. From the completions of B and C at their augmentation ideals, we obtain two-dimensional polynomial formal groups $\mathscr{F}$ and $\mathscr{G}$, respectively. The flat epimorphism Θ will then translate to an isogeny Ψ: $\mathscr{F} \to \mathscr{G}$ with kernel Spec $H_v(i, j)$. We begin with some preliminaries on forma groups.

1. FORMAL GROUPS

An *n-dimensional formal group (law)* $\mathscr{F}$ is an n-tuple of power series,

$$\mathscr{F}(\bar{x}, \bar{y}) = (\mathscr{F}_1(\bar{x}, \bar{y}), \ldots, \mathscr{F}_n(\bar{x}, \bar{y})),$$

in the variables $\bar{x} = (x_1, \ldots, x_n)$, $\bar{y} = (y_1, \ldots, y_n)$, satisfying the conditions,

$$\mathscr{F}_i(\bar{x}, \bar{y}) \equiv x_i + y_i \ (\text{mod degree } 2)$$

and

$$\mathscr{F}_i(\mathscr{F}(\bar{x}, \bar{y}), \bar{z}) = \mathscr{F}_i(\bar{x}, \mathscr{F}(\bar{y}, \bar{z})),$$

for $i = 1, \ldots, n$. The formal group $\mathscr{F}$ is *commutative* if $\mathscr{F}_i(\bar{x}, \bar{y}) = \mathscr{F}_i(\bar{y}, \bar{x})$ for $i = 1, \ldots, n$. $\mathscr{F}$ is a *polynomial formal group* if the power series $\mathscr{F}_i(\bar{x}, \bar{y})$ are polynomials. A *homomorphism* Ψ: $\mathscr{F} \to \mathscr{G}$ of formal groups is an n-tuple of power series,

$$\Psi(\bar{x}) = (\Psi_1(\bar{x}), \ldots, \Psi_n(\bar{x}))$$

satisfying $\Psi_i(\bar{0}) = \bar{0}$, $\Psi_i(\mathscr{F}(\bar{x}, \bar{y})) = \mathscr{G}_i(\Psi(\bar{x}), \Psi(\bar{y}))$ for $i = 1, \ldots, n$. Ψ is an *isogeny* of formal groups if $R[[X]]/\langle \Psi_1(X), \ldots, \Psi_n(X)\rangle$ is a finite R-algebra where $R[[X]] = R[[X_1, \ldots, X_n]]$ denotes the R-algebra of power series in n-variables.

A given formal group $\mathscr{F}$ induces a *formal Hopf algebra* structure on $R[[X]]$: The comultiplication map $\Delta\colon R[[X]] \to R[[X]] \hat{\otimes} R[[X]]$ is defined $\Delta(X_i) = \mathscr{F}_i(X \hat{\otimes} 1, 1 \hat{\otimes} X)$, for $i = 1, \ldots, n$. (Here $\hat{\otimes}$ denotes the completion of the tensor product.) The counit map $\epsilon\colon R[[X]] \to R$ is given $\epsilon(X_i) = 0$, and the coinverse map $\sigma\colon R[[X]] \to R[[X]]$ is defined $X \mapsto \sigma(X)$, where $\sigma(X)$ is the unique power series satisfying $\mathscr{F}(X, \sigma(X)) = 0$, cf. [3, p. 4]. If $\Psi\colon \mathscr{F} \to \mathscr{G}$ is an isogeny of formal groups, then the quotient

$$\frac{R[[X]]}{\langle \Psi_1(X), \ldots, \Psi_n(X)\rangle} = R[[x]], \qquad (x = \bar{X})$$

is a finite R-Hopf algebra via the maps $\Delta\colon R[[x]] \to R[[x]] \otimes R[[x]]$ defined $\Delta(x_i) = \mathscr{F}_i(x \otimes 1, 1 \otimes x)$, $\epsilon\colon R[[x]] \to R$, given $\epsilon(x_i) = 0$ and $\sigma\colon R[[x]] \to R[[x]]$ defined $x \mapsto \sigma(x)$. In this case, Spec $R[[x]]$ is the *kernel* of the isogeny, equivalently, $R[[x]]$ represents the kernel of Ψ.

If Ψ is an isogeny $\mathscr{F} \to \mathscr{G}$ and $\mathscr{F}$ is a polynomial formal group, then $\mathscr{F}$ endows $R[X]$ with the structure of an ordinary R-bialgebra via the maps $\Delta\colon R[X] \to R[X] \otimes R[X]$ defined $\Delta(X_i) = \mathscr{F}_i(X \otimes 1, 1 \otimes X)$ and $\epsilon\colon R[X] \to R$ defined $\epsilon(X_i) = 0$ for $i = 1, \ldots, n$. We denote this R-bialgebra by $R[X]_{\mathscr{F}}$. In this case, Ψ and $\mathscr{F}$ determine a finite R-Hopf algebra structure on the quotient,

$$\frac{R[X]_{\mathscr{F}}}{\langle \Psi_1(X), \ldots, \Psi_n(X)\rangle} = R[x], \qquad (x = \bar{X}).$$

For example, let $\mathscr{F}$ and $\mathscr{G}$ be one-dimensional commutative polynomial formal groups defined

$$\mathscr{F}(x, y) = x + y + \pi^i xy, \quad \text{and} \quad \mathscr{G}(x, y) = x + y + \pi^{pi} xy,$$

where i is an integer, $0 \le i \le e/(p-1)$. Because $i \le e/(p-1)$, the polynomial $\Psi(x) = [(1 + \pi^i x)^p - 1]/\pi^{pi}$ is monic with coefficients in R. Thus $\Psi\colon \mathscr{F} \to \mathscr{G}$ is an isogeny of polynomial formal groups. The associated finite R-Hopf algebra $R[X]_{\mathscr{F}}/\langle \Psi(X)\rangle$ is isomorphic to the Larson order,

$$H(i) = R\left[\frac{g^p - 1}{\pi^i}\right] \subseteq KC_p, \qquad \langle g\rangle = C_{p^2}.$$

(See [5, 13] for details on Larson orders.) Thus Spec $H(i)$ is the kernel of Ψ, [1, pp. 11–15].

2. POLYNOMIAL FORMAL GROUPS AND HOPF ORDERS

In this section we show that under certain conditions, the comultiplication of R-Hopf orders in KC_{p^2} is determined by two-dimensional commutative polynomial formal groups which we can compute explicitly. These formal groups are necessarily of the form given by Childs *et al.* [2, Proposition 1.1] in the following classification theorem.

THEOREM 2.0 (Childs *et al.*). *Let $\mathscr{F}$ be a two-dimensional commutative polynomial formal group. Then*

$$\mathscr{F}(\bar{x},\bar{y}) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} a & ch \\ dh & df \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_1 + \begin{pmatrix} ch & cf \\ df & b \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_2,$$

for some elements $a, b, c, d, f, h \in R$ satisfying $af + bh = ch^2 + df^2$. Here

$$\mathscr{F}_1(\bar{x},\bar{y}) = x_1 + y_1 + ax_1y_1 + chx_2y_1 + chx_1y_2 + cfx_2y_2,$$

and

$$\mathscr{F}_2(\bar{x},\bar{y}) = x_2 + y_2 + dhx_1y_1 + dfx_2y_1 + dfx_1y_2 + bx_2y_2.$$

We first show that the comultiplication of the Larson order $H(i, j) = R[(g^p - 1)/\pi^i, (g - 1)/\pi^j]$ in KC_{p^2} is dictated by a certain two-dimensional polynomial formal group. (Here $i, j \in \mathbf{Z}$ with $0 \le i, j \le e/(p - 1)$, $pj \le i$.) Comultiplication in $H(i, j)$ is defined

$$\Delta\left(\frac{g^p - 1}{\pi^i}\right) = \left(\frac{g^p - 1}{\pi^i}\right) \otimes 1 + 1 \otimes \left(\frac{g^p - 1}{\pi^i}\right) + \pi^i\left(\frac{g^p - 1}{\pi^i}\right) \otimes \left(\frac{g^p - 1}{\pi^i}\right),$$

$$\Delta\left(\frac{g - 1}{\pi^j}\right) = \left(\frac{g - 1}{\pi^j}\right) \otimes 1 + 1 \otimes \left(\frac{g - 1}{\pi^j}\right) + \pi^j\left(\frac{g - 1}{\pi^j}\right) \otimes \left(\frac{g - 1}{\pi^j}\right).$$

Put $a_1 = ((g^p - 1)/\pi^i) \otimes 1$, $b_1 = 1 \otimes ((g^p - 1)/\pi^i)$, $a_2 = ((g - 1)/\pi^j) \otimes 1$, and $b_2 = 1 \otimes ((g - 1)/\pi^j)$, with $\bar{a} = (a_1, a_2)$, $\bar{b} = (b_1, b_2)$. Then

$$\Delta\left(\frac{g^p - 1}{\pi^i}\right) = \mathscr{F}_1(\bar{a},\bar{b}) \quad \text{and} \quad \Delta\left(\frac{g - 1}{\pi^j}\right) = \mathscr{F}_2(\bar{a},\bar{b}),$$

where $\mathscr{F}_1, \mathscr{F}_2$ are polynomials defined $\mathscr{F}_1(\bar{x},\bar{y}) = x_1 + y_1 + \pi^i x_1 y_1$ and $\mathscr{F}_2(\bar{x},\bar{y}) = x_2 + y_2 + \pi^j x_2 y_2$, $\bar{x} = (x_1, x_2)$, $\bar{y} = (y_1, y_2)$ indeterminate.

One easily checks that these polynomials define a two-dimensional polynomial formal group $\mathscr{F}(\mathscr{F}_1, \mathscr{F}_2)$. In this sense, the formal group $\mathscr{F}$ determines the comultiplication of $H(i, j)$. In matrix form $\mathscr{F}$ appears as

$$\mathscr{F}(\bar{x}, \bar{y}) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} \pi^i & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_1 + \begin{pmatrix} 0 & 0 \\ 0 & \pi^j \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_2. \quad (2.1)$$

Moreover, a different polynomial formal group prescribes the comultiplication of non-Larson R-Hopf orders in KC_{p^2} under certain conditions. Let π^i and π^j be elements of R with i and j satisfying $i + j \leq e/(p-1)$, and $pj \leq i$. Recall $i' = e/(p-1) - i$, e is the ramification index of p in R, and $U_n = \{x \in R | x \in 1 + \pi^n R\}$, for integers $n \geq 0$. A class $[v]$ in $(U_{i'+(j/p)} \cap U_{(i'/p)+j})/U_{i'+j}$ corresponds to an R-Hopf order in KC_{p^2} of the form,

$$H_v(i, j) = R\left[\frac{g^p - 1}{\pi^i}, \frac{g - a_v}{\pi^j}\right]$$

called a Greither order, see [4, Corollary I.3.6]. In this case, the condition $i + j \leq e/(p-1)$ implies

$$i' + \frac{j}{p} \geq \frac{i'}{p} + j,$$

thus the class $[v]$ may be taken from the quotient $U_{i'+(j/p)}/U_{i'+j}$. The quantity $a_v \in H(i)$ is of the form $a_v = \sum_{m=0}^{p-1} v^m f_m$, where the f_m are the idempotents for the maximal integral order in KC_p, $f_m = 1/p \sum_{n=0}^{p-1} \zeta_1^{-mn} g^{pn}$, $\langle g \rangle = C_{p^2}$. Let us suppose further that

$$i' + \frac{j}{2} \leq \nu(1 - v) < i' + j,$$

that is, $v \in U_{i'+(j/2)}$ and $v \notin U_{i'+j}$. (If $v \in U_{i'+j}$, then $H_v(i, j)$ is the Larson order $H(i, j)$.) Under such conditions the comultiplication of $H_v(i, j)$ is determined by a commutative polynomial formal group. We begin with a lemma.

LEMMA 2.2. *Under the conditions set forth in the previous text, the Greither order* $H_v(i, j) = R[(g^p - 1)/\pi^i, (g - a_v)/\pi^j]$ *can be written*

$$H_v(i, j) = R\left[\frac{g^p - 1}{\pi^i}, \frac{g - 1}{\pi^j} + \frac{g^p - 1}{\lambda \pi^i}\right],$$

where $\lambda = \pi^{j-i}((\zeta_1 - 1)/(1 - v))$.

Proof. First decompose the algebra generator $(g - a_v)/\pi^j$ of $H_v(i, j)$,

$$\begin{aligned}\frac{g - a_v}{\pi^j} &= \frac{g - 1}{\pi^j} + \frac{1 - a_v}{\pi^j} \\ &= \frac{g - 1}{\pi^j} + \frac{1}{\pi^j}\left[(1 - v)f_1 + (1 - v^2)f_2 + \cdots + (1 - v^{p-1})f_{p-1}\right] \\ &= \frac{g - 1}{\pi^j} + \frac{(1 - v)(g^p - 1)}{(\zeta_1 - 1)\pi^j}\Omega.\end{aligned}$$

Here ζ_1 is a primitive pth root of unity, the f_m are idempotents for the maximal integral order in KC_p, and

$$\begin{aligned}\Omega = f_1 + \left(\frac{\zeta_1 - 1}{\zeta_1^2 - 1}\right)(1 + v)f_2 + \cdots + \left(\frac{\zeta_1 - 1}{\zeta_1^{p-1} - 1}\right) \\ \times(1 + v + \cdots + v^{p-2})f_{p-1}.\end{aligned}$$

We claim that

$$\frac{(1 - v)(g^p - 1)}{(\zeta_1 - 1)\pi^j}\Omega - \frac{(1 - v)(g^p - 1)}{(\zeta_1 - 1)\pi^j} \in H(i) = R\left[\frac{g^p - 1}{\pi^i}\right].$$

To this end, let

$$\Lambda = \frac{(1 - v)(g^p - 1)}{(\zeta_1 - 1)\pi^j}(\Omega - 1),$$

and let

$$\begin{aligned}\xi = \Bigg(0, 0, \frac{(1 - v)(\zeta_1^2 - 1)}{(\zeta_1 - 1)\pi^j}\left(\frac{\zeta_1 - 1}{\zeta_1^2 - 1}(1 + v) - 1\right), \\ \ldots, \frac{(1 - v)(\zeta_1^{p-1} - 1)}{(\zeta_1 - 1)\pi^j}\left(\frac{\zeta_1 - 1}{\zeta_1^{p-1} - 1}(1 + v + \cdots + v^{p-1}) - 1\right)\Bigg)\end{aligned}$$

be the embedding of Λ into the maximal integral order R^p in KC_{p^2}. (The embedding is defined $g^p \mapsto (1, \zeta_1, \zeta_1^2, \ldots, \zeta_1^{p-1})$.) Now consider the kth iterated difference of ξ, denoted $d^k(\xi)$, see [4, Section I.3]. We have $d^1(\xi) = 0$,

$$\begin{aligned}d^2(\xi) &= \frac{(1 - v)(v - \zeta_1)}{\pi^j}, \\ d^k(\xi) &= \frac{(1 - v)(v - \zeta_1)}{\pi^j}\sum_{m+n=k-2}(1 - \zeta_1)^m(1 - v)^n,\end{aligned}$$

for $2 \le k \le p-1$. Thus,

$$\begin{aligned}\nu(d^k(\xi)) &\ge \nu(1-v) + \nu(v-\zeta_1) + (k-2)\nu(1-v) - j \\ &= k\nu(1-v) - j,\end{aligned}$$

because $\nu(1-\zeta_1) > \nu(1-v)$. Now because $\nu(1-v) \ge i' + (j/2)$,

$$\begin{aligned}\nu(d^k(\xi)) &\ge ki' + \frac{kj}{2} - j \\ &\ge ki'\end{aligned}$$

for $k = 2, \dots, p-1$. Thus by [4, Theorem I.3.2(a)], Λ is in $H(i)$. We conclude that the R-Hopf order $R[(g^p-1)/\pi^i, (g-a_v)/\pi^j]$ is equal to the R-Hopf order,

$$R\left[\frac{g^p-1}{\pi^i}, \frac{g-1}{\pi^j} + \frac{(1-v)(g^p-1)}{(\zeta_1-1)\pi^j}\right].$$

Now let $\lambda = \pi^{j-i}((\zeta_1-1)/(1-v))$ then

$$\frac{g-1}{\pi^j} + \frac{(1-v)(g^p-1)}{(\zeta_1-1)\pi^j} = \frac{g-1}{\pi^j} + \frac{g^p-1}{\lambda\pi^i}.$$

This completes the proof of the lemma. ∎

THEOREM 2.3. *Suppose* $0 \le i,\ j \le e/(p-1)$, $i+j \le e/(p-1)$, *and* $pj \le i$. *Then a class* $[v]$ *in* $U_{i'+(j/p)}/U_{i'+j}$ *with* $i'+j > \nu(1-v) \ge i' + (j/2)$ *corresponds to a Greither order* $H_v(i,j) = R[(g^p-1)/\pi^i, (g-a_v)/\pi^j]$ *in* KC_{p^2}. *Moreover, there exists a polynomial formal group of the form,*

$$\begin{aligned}\mathscr{F}(\bar{x},\bar{y}) = \begin{pmatrix}x_1\\x_2\end{pmatrix} + \begin{pmatrix}y_1\\y_2\end{pmatrix} + \begin{pmatrix}\pi^i & 0\\ \dfrac{\pi^i\lambda + \pi^j}{\lambda^2} & \dfrac{-\pi^j}{\lambda}\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}y_1 \\ + \begin{pmatrix}0 & 0\\ \dfrac{-\pi^j}{\lambda} & \pi^j\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}y_2,\end{aligned} \tag{2.4}$$

with $\lambda = \pi^{j-i}((\zeta_1-1)/(1-v))$, *which determines the comultiplication of* $H_v(i,j)$.

Proof. By Lemma 2.2,

$$H_v(i,j) = R\left[\frac{g^p - 1}{\pi^i}, \frac{g-1}{\pi^j} + \frac{g^p - 1}{\lambda\pi^i}\right].$$

Setting $A = (g^p - 1)/\pi^i$, $B = (g-1)/\pi^j$, we have $H_v(i,j) = R[A, B + (1/\lambda)A]$, with

$$\Delta(A) = A \otimes 1 + 1 \otimes A + \pi^i A \otimes A,$$

$$\Delta\left(B + \frac{1}{\lambda}A\right) = B \otimes 1 + 1 \otimes B + \pi^j B \otimes B + \frac{1}{\lambda}(A \otimes 1)$$

$$+ \frac{1}{\lambda}(1 \otimes A) + \frac{\pi^i}{\lambda} A \otimes A.$$

Now put $m_1 = A \otimes 1$, $n_1 = 1 \otimes A$, $m_2 = B \otimes 1$, $n_2 = 1 \otimes B$, $\bar{m} = (m_1, m_2)$, $\bar{n} = (n_1, n_2)$. Then comultiplication in $H_v(i,j)$ is determined by a two-dimensional formal group $\mathscr{S}(\mathscr{S}_1, \mathscr{S}_2)$ defined

$$\mathscr{S}_1(\bar{u}, \bar{z}) = u_1 + z_1 + \pi^i u_1 z_1,$$

$$\mathscr{S}_2(\bar{u}, \bar{z}) = u_2 + z_2 + \pi^j u_2 z_2 + \frac{1}{\lambda}u_1 + \frac{1}{\lambda}z_1 + \frac{\pi^i}{\lambda}u_1 z_1$$

$$= \left(u_2 + \frac{1}{\lambda}u_1\right) + \left(z_2 + \frac{1}{\lambda}z_1\right) + \pi^j u_2 z_2 + \frac{\pi^i}{\lambda}u_1 z_1,$$

$\bar{u} = (u_1, u_2)$, $\bar{z} = (z_1, z_2)$ indeterminate, that is, $\Delta(A) = \mathscr{S}_1(\bar{m}, \bar{n})$, and $\Delta(B + \lambda^{-1}A) = \mathscr{S}_2(\bar{m}, \bar{n})$. In matrix form $\mathscr{S}$ appears as

$$\mathscr{S}(\bar{u}, \bar{z}) = \begin{pmatrix} u_1 \\ u_2 + \frac{1}{\lambda}u_1 \end{pmatrix} + \begin{pmatrix} z_1 \\ z_2 + \frac{1}{\lambda}z_1 \end{pmatrix} + \begin{pmatrix} \pi^i & 0 \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 + \frac{1}{\lambda}u_1 \end{pmatrix} z_1$$

$$+ \begin{pmatrix} 0 & 0 \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 + \frac{1}{\lambda}u_1 \end{pmatrix} \left(z_2 + \frac{1}{\lambda}z_1\right).$$

Here $\alpha, \beta, \gamma, \delta$ are elements in R so that the formula for $\mathscr{S}_2$ given in the preceding text is satisfied. It follows that

$$\alpha u_1 z_1 + \beta\left(u_2 + \frac{1}{\lambda}u_1\right)z_1 + \gamma u_1\left(z_2 + \frac{1}{\lambda}z_1\right) + \delta\left(u_2 + \frac{1}{\lambda}u_1\right)\left(z_2 + \frac{1}{\lambda}z_1\right)$$

$$= \pi^j u_2 z_2 + \frac{\pi^i}{\lambda}u_1 z_1.$$

Thus we have a system of equations,

$$\begin{aligned}\alpha+\frac{\beta}{\lambda}+\frac{\gamma}{\lambda}+\frac{\delta}{\lambda^2}&=\frac{\pi^i}{\lambda},\\ \beta+\frac{\delta}{\lambda}&=0,\\ \gamma+\frac{\delta}{\lambda}&=0,\\ \delta&=\pi^j,\end{aligned}$$

with a unique solution,

$$\alpha=\frac{\pi^i\lambda+\pi^j}{\lambda^2},\qquad \beta=\gamma=\frac{-\pi^j}{\lambda},\qquad \delta=\pi^j.$$

Now with $x_1=u_1,\ y_1=z_1,\ x_2=u_2+(1/\lambda)u_1,\ y_2=z_2+(1/\lambda)z_1$, we have the polynomial formal group $\mathscr{F}$ in matrix form,

$$\mathscr{F}(\bar{x},\bar{y})=\begin{pmatrix}x_1\\x_2\end{pmatrix}+\begin{pmatrix}y_1\\y_2\end{pmatrix}+\begin{pmatrix}\pi^i & 0\\ \dfrac{\pi^i\lambda+\pi^j}{\lambda^2} & \dfrac{-\pi^j}{\lambda}\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}y_1$$
$$+\begin{pmatrix}0 & 0\\ \dfrac{-\pi^j}{\lambda} & \pi^j\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}y_2.$$

Indeed, setting $a=\pi^i$, $b=\pi^j$, $ch=0$, $dh=(\pi^i\lambda+\pi^j)/\lambda^2$, and $df=(-\pi^j)/\lambda$ we have

$$\begin{aligned}af+bh&=\frac{-\pi^i\pi^j}{\lambda d}+\frac{\pi^j\pi^i\lambda+\pi^{2j}}{\lambda^2 d}\\ &=\frac{\pi^{2j}}{\lambda^2 d}\\ &=ch^2+df^2,\end{aligned}$$

as required by Theorem 2.0.

Observe that $\Delta(A)=\mathscr{F}_1(\overline{M},\overline{N})$ and $\Delta(B+\lambda^{-1}A)=\mathscr{F}_2(\overline{M},\overline{N})$, with $\overline{M}=(m_1,m_2+\lambda^{-1}m_1)$, $\overline{N}=(n_1,n_2+\lambda^{-1}n_1)$, thus $\mathscr{F}$ determines the comultiplication of $H_v(i,j)$. ∎

3. A FLAT RESOLUTION OF Spec $H_v(i,j)$

In this section we give an explicit resolution of Spec $H_v(i,j)$ from which we construct our isogeny of polynomial formal groups with kernel Spec $H_v(i,j)$ (Sections 4 and 5). As before, $H_v(i,j)$ is a Greither order under the conditions $i' + j > \nu(1-v) \geq i' + (j/2)$ and $i + j \leq e/(p-1)$. There exists a flat short exact sequence of R-group schemes,

$$\text{Spec } H_v(i,j) \to W_{i,j} \xrightarrow{\Theta} V_{pi,pj}.$$

Here the group scheme $W_{i,j}$ is represented by the R-Hopf algebra,

$$B = R\Big[T_0, T_1, \big(1+\pi^i T_0\big)^{-1}, \big(F(T_0)+\pi^j T_1\big)^{-1}\Big],$$

and the group scheme $V_{pi,pj}$ is represented by the R-Hopf algebra,

$$C = R\Big[T_0, T_1, \big(1+\pi^{pi} T_0\big)^{-1}, \big(G(T_0)+\pi^{pj} T_1\big)^{-1}\Big],$$

for some polynomials $F(T_0), G(T_0) \in R[T_0]$ satisfying

$$F(0) = 1 \quad \text{and} \quad F(X)F(Y) \equiv F(X+Y+\pi^i XY) \pmod{\pi^j}, \tag{3.0}$$

and

$$G(0) = 1 \quad \text{and} \quad G(X)G(Y) \equiv G(X+Y+\pi^{pi}XY) \pmod{\pi^{pj}}, \tag{3.1}$$

X, Y indeterminate. The flat epimorphism Θ is defined $\Theta(T_0, T_1) = (\Theta_0(T_0), \Theta_1(T_0, T_1))$ with

$$\Theta_0(T_0) = \frac{\big(1+\pi^i T_0\big)^p - 1}{\pi^{pi}},$$

$$\Theta_1(T_0, T_1) = \frac{\big(1+\pi^i T_0\big)^{-1}\big(F(T_0)+\pi^j T_1\big)^p - G\big(\Theta_0(T_0)\big)}{\pi^{pj}}.$$

Moreover, Spec $H_v(i,j)$ is the kernel of Θ, that is, $B/\langle \Theta_0(T_0), \Theta_1(T_0,T_1)\rangle \cong H_v(i,j)$, cf. [10, Proposition 2.2; 15, Lemma 3.0].

We intend to give an explicit description of the flat epimorphism Θ and the representing R-Hopf algebras B and C of the group schemes $W_{i,j}$ and $V_{pi,pj}$. First note the polynomial $F(T_0)$ can be modeled from the structure of a_v, that is, we may choose

$$F(T_0) = F_v(T_0) = \frac{1}{p}\sum_{m=0}^{p-1} v^m \sum_{n=0}^{p-1} \zeta_1^{-mn}\big(1+\pi^i T_0\big)^n. \tag{3.2}$$

cf. [15, Lemma 3.0]. With this choice of $F(T_0)$, Spec B is a group scheme. Observe that comultiplication on the R-Hopf algebra B is the unique R-algebra map which makes the quantities $1 + \pi^i T_0$ and $F_v(T_0) + \pi^j T_1$ grouplike.

We claim that a polynomial $G(T_0)$ for which Spec C is a group scheme can be constructed directly from $F_v(T_0)$, as follows. Let $\alpha(T_0)$ be any polynomial in $R[T_0, (1 + \pi^i T_0)^{-1}]$, with $\deg(\alpha) \le kp$, for some $k \in \mathbf{Z}^+$. Put $\alpha(T_0)$ in the form,

$$\alpha(T_0) = \sum_{m=0}^{kp} a_m \big(1 + \pi^i T_0\big)^m, \qquad a_m \in K,$$

and write the polynomial,

$$\begin{aligned} &M\big(\alpha(T_0)\big) \\ &\quad = (a_0 + a_1 + a_2 + \cdots + a_{p-1}) + (a_p + \cdots + a_{2p-1})\big(1 + \pi^i T_0\big)^p \\ &\qquad + (a_{2p} + \cdots + a_{3p-1})\big(1 + \pi^i T_0\big)^{2p} + \cdots \\ &\qquad + (a_{(k-1)p} + \cdots + a_{k_{p-1}})\big(1 + \pi^i T_0\big)^{(k-1)p} \\ &\qquad + a_{k_p}\big(1 + \pi^i T_0\big)^{kp}. \end{aligned}$$

Note that $M(\alpha(T_0))$ can be viewed as the polynomial $\beta(\Theta_0(T_0))$ with

$$\begin{aligned} \beta(T_0) &= (a_0 + a_1 + a_2 + \cdots + a_{p-1}) + (a_p + \cdots + a_{2p-1})\big(1 + \pi^{pi} T_0\big) \\ &\quad + (a_{2p} + \cdots + a_{3p-1})\big(1 + \pi^{pi} T_0\big)^2 + \cdots \\ &\quad + (a_{(k-1)p} + \cdots + a_{kp-1})\big(1 + \pi^{pi} T_0\big)^{k-1} \\ &\quad + a_{kp}\big(1 + \pi^{pi} T_0\big)^k. \end{aligned}$$

We designate this polynomial $\beta(T_0)$ by $N(M(\alpha(T_0)))$. We claim that if

$$G(T_0) = G_v(T_0) = N\Big(M\big(F_v(T_0)^p\big)\Big), \tag{3.3}$$

with $F_v(T_0)$ as in (3.2), then the R-algebra,

$$C = R\Big[T_0, T_1, \big(1 + \pi^{pi} T_0\big)^{-1}, \big(G_v(T_0) + \pi^{pj} T_1\big)^{-1}\Big]$$

is an R-Hopf algebra. We show that C is an Hopf algebra (Theorem 3.9) by showing that $G_v(T_0) = N(M(F_v(T_0)^p))$ satisfies condition (3.1). We begin with some lemmas about M.

LEMMA 3.4. *The epimorphism* $\Theta_0(T_0)$ *may be written as* $M(T_0^p)$.

Proof. We compute directly,

$$\begin{aligned} M(T_0^p) &= M\left(\left(\frac{(1+\pi^i T_0)-1}{\pi^i}\right)^p\right) \\ &= M\left(\frac{1}{\pi^{pi}}\left((1+\pi^i T_0)^p - \binom{p}{1}(1+\pi^i T_0)^{p-1} \cdots \right.\right. \\ &\qquad \left.\left. + \binom{p}{p-1}(1+\pi^i T_0) - 1\right)\right) \\ &= \frac{1}{\pi^{pi}}\left((1+\pi^i T_0)^p - 1\right) \\ &= \Theta_0(T_0). \end{aligned}$$

∎

LEMMA 3.5. *Suppose* α, β *are two polynomials in* $R[T_0, (1+\pi^i T_0)^{-1}]$. *Then the following holds*:

i. $M(\alpha) \in R[T_0, (1+\pi^i T_0)^{-1}]$
ii. *For any* $r \in R$, $M(r\alpha(T_0)) = rM(\alpha(T_0))$
iii. $M(\alpha+\beta) = M(\alpha) + M(\beta)$.

Proof. Conditions i.–iii. follow immediately from the definition of M.

∎

Now suppose $\alpha(X,Y)$ is a polynomial in $R[X,Y]$, X, Y indeterminate, in the form

$$\alpha(X,Y) = \sum_{m=0}^{k}\sum_{n=0}^{l} a_{mn}(1+\pi^i X)^n (1+\pi^i Y)^n, \qquad a_m \in K.$$

In view of Lemma 3.5, we define $M(\alpha(X,Y))$ as

$$M(\alpha(X,Y)) = \sum_{m=0}^{k}\sum_{n=0}^{l} a_{mn} M\left((1+\pi^i X)^m\right) M\left((1+\pi^i Y)^n\right). \quad (3.6)$$

Observe that definition (3.6) implies that $M(\alpha(X,Y)) \in R[X,Y]$ whenever $\alpha(X,Y) \in R[X,Y]$.

LEMMA 3.7. *Suppose* $\alpha(X)$, $\beta(Y)$ *are polynomials in* $R[X,Y]$. *Then*

$$M(\alpha(X)\beta(Y)) = M(\alpha(X))M(\beta(Y)).$$

Proof. Write $\alpha(X) = \sum_{m=0}^{k} a_m(1 + \pi^i X)^m$, $\beta(Y) = \sum_{n=0}^{l} b_n(1 + \pi^i Y)^n$, $a_m, b_n \in K$. Then $\alpha\beta$ is a polynomial,

$$\sum_{m=0}^{k} \sum_{n=0}^{l} a_{mn}(1 + \pi^i X)^m (1 + \pi^i Y)^n,$$

in $R[X, Y]$. Thus by definition (3.6),

$$\begin{aligned} M(\alpha\beta) &= \sum_{m=0}^{k} \sum_{n=0}^{l} a_{mn} M\big((1 + \pi^i X)^m\big) M\big((1 + \pi^i Y)^n\big) \\ &= \left(\sum_{m=0}^{k} a_m M\big((1 + \pi^i X)^m\big) \right) \left(\sum_{n=0}^{l} b_n M\big((1 + \pi^i Y)^n\big) \right) \\ &= M(\alpha) M(\beta), \end{aligned}$$

by Lemma 3.5. ∎

LEMMA 3.8. *Let X and Y be indeterminates. Then*

$$M\big(F_v(X + Y + \pi^i XY)^p\big) \equiv M\big(F_v(X)^p\big) M\big(F_v(Y)^p\big) \pmod{\pi^{pj}}.$$

Proof. Using (3.0) write

$$F_v(X + Y + \pi^i XY) = F_v(X) F_v(Y) + \pi^j q(X, Y),$$

for some polynomial $q(X, Y)$ with coefficients in R. Taking pth powers of both sides yields

$$F_v(X + Y + \pi^i XY)^p = F_v(X)^p F_v(Y)^p + \pi^{pj} q'(X, Y),$$

for some polynomial $q'(X, Y)$ over R because $e + j \geq pj$. Applying M and definition (3.6) yields

$$\begin{aligned} M\big(F_v(X + Y + \pi^i XY)^p\big) &= M\big(F_v(X)^p F_v(Y)^p + \pi^{pj} q'(X, Y)\big) \\ &= M\big(F_v(X)^p F_v(Y)^p\big) + \pi^{pj} q''(X, Y), \end{aligned}$$

for some $q''(X, Y)$ over R. Now by Lemma 3.7,

$$M\big(F_v(X)^p F_v(Y)^p\big) = M\big(F_v(X)^p\big) M\big(F_v(Y)^p\big),$$

thus $M(F_v(X + Y + \pi^i XY)^p)$ is congruent modulo π^{pj} to $M(F_v(X)^p)$ $M(F_v(Y)^p)$. ∎

We are now in a position to prove the following theorem.

THEOREM 3.9. *Let C be the R-algebra,*

$$C = R\Big[T_0, T_1, \big(1 + \pi^{pi}T_0\big)^{-1}, \big(G_v(T_0) + \pi^{pj}T_1\big)^{-1}\Big],$$

with

$$G_v(T_0) = N\big(M\big(F_v(T_0)^p\big)\big),$$

with $F_v(T_0)$ as in (3.2). *Then* Spec C *is a group scheme.*

Proof. We show directly that Spec $C(A) = \mathrm{Hom}_{R-\mathrm{alg}}(C, A)$ is an abstract group for any commutative R-algebra A. Observe that Spec $C(A)$ is a group if and only if the conditions

i. $G_v(0) = 1$ and

ii. $G_v(S)G_v(T) \equiv G_v(S * T) \pmod{\pi^{pj}A}$

hold. Here $S, T \in \mathrm{Spec}\, R[T_0, (1 + \pi^{pi}T_0)^{-1}](A)$ and $S * T = S + T + \pi^{pi}ST$ is the group product of the points S, T. (Actually, S, T are elements of A that are identified with maps $T_0 \mapsto S$, $T_0 \mapsto T$ in Spec $R[T_0, (1 + \pi^{pi}T_0)^{-1}](A)$.) We have $G_v(0) = G_v(\Theta_0(0)) = M(F_v(0)^p) = M(1) = 1$ thus condition i. is satisfied. Recall the epimorphism,

$$\Theta_0(T_0)\colon \mathrm{Spec}\, R\Big[T_0, \big(1 + \pi^{i}T_0\big)^{-1}\Big] \to \mathrm{Spec}\, R\Big[T_0, \big(1 + \pi^{pi}T_0\big)^{-1}\Big],$$

in the flat topology, see [4, Lemma I.1.2]. There exists a commutative R-algebra $A' \supseteq A$ and elements $W, Z, W \neq Z$ in Spec $R[T_0, (1 + \pi^{i}T_0)^{-1}](A')$ so that $S = \Theta_0(W)$ and $T = \Theta_0(Z)$. Then

$$\begin{aligned} G_v(S)G_v(T) &= G_v(\Theta_0(W))G_v(\Theta_0(Z)) = M\big(F_v(W)^p\big)M\big(F_v(Z)^p\big) \\ &\equiv M\big(F_v(W + Z + \pi^{i}WZ)^p\big) \pmod{\pi^{pj}A'}, \end{aligned}$$

by Lemma 3.8. Note $W + Z + \pi^{i}WZ$ is the group product in Spec $R[T_0, (1 + \pi^{i}T_0)^{-1}](A')$, denoted $W \bigstar Z$, thus

$$\begin{aligned} M\big(F_v(W + Z + \pi^{i}WZ)^p\big) &= M\big(F_v(W \bigstar Z)^p\big) \\ &= G_v(\Theta_0(W \bigstar Z)) \\ &= G_v(\Theta_0(W) * \Theta_0(Z)) \\ &= G_v(S * T), \end{aligned}$$

because Θ_0 is a group homomorphism. Thus $G_v(S)G_v(T) \equiv G_v(S * T) \pmod{\pi^{pj}A}$. It follows Spec C is a group scheme. Moreover, comultiplication on the R-Hopf algebra C is the unique R-algebra map which makes $1 + \pi^{pi}T_0$ and $G_v(T_0) + \pi^{pj}T_1$ grouplike. ∎

Remark 3.10. The choice of the polynomial $G(T_0)$ so that Spec C is a group scheme is not unique. For example, we could have chosen $G(T_0) = N(M'(F_v(T_0)^p))$, where

$$\begin{aligned} M'(\alpha(T_0)) = a_0 &+ (a_1 + a_2 + \cdots + a_p)(1 + \pi^i T_0)^p \\ &+ (a_{p+1} + \cdots + a_{2p})(1 + \pi^i T_0)^{2p} \\ &+ (a_{2p+1} + \cdots + a_{3p})(1 + \pi^i T_0)^{3_p} + \cdots \\ &+ (a_{(k-1)p+1} + \cdots + a_{kp})(1 + \pi^i T_0)^{kp}, \end{aligned}$$

and N is defined as before.

Now that we have explicit forms for the group schemes Spec B and Spec C, we show that the map Θ: Spec $B \to$ Spec C, defined $\Theta(T_0, T_1) = (\Theta_0(T_0), \Theta_1(T_0, T_1))$ with

$$\Theta_0(T_0) = \frac{(1 + \pi^i T_0)^p - 1}{\pi^{pi}},$$

$$\Theta_1(T_0, T_1) = \frac{(1 + \pi^i T_0)^{-1}(F_v(T_0) + \pi^j T_1)^p - G_v(\Theta_0(T_0))}{\pi^{pj}}$$

is a flat epimorphism of group schemes. But this is equivalent to showing that the polynomials Θ_0 and Θ_1 have coefficients in R, see [6, p. 63, Theorem 2.15(c)]. It is easy to show that $i \le e/(p-1)$ implies $\Theta_0 \in R[T_0]$. We claim that

$$\Theta_1(T_0, T_1) = \frac{(1 + \pi^i T_0)^{-1}(F_v(T_0) + \pi^j T_1)^p - G_v(\Theta_0(T_0))}{\pi^{pj}}$$

has coefficients in R. To this end, let $F_{m,R}$ be the subset of the multiplicative group $G_{m,R}$ defined

$$\begin{aligned} F_{m,R}(A) = \Big\{ u \in U(A) | u = F_v(a) + \pi^j t \text{ for some } t \in A, \\ a \in \text{Spec } R\Big[T_0, (1 + \pi^i T_0)^{-1}\Big](A) \Big\}. \end{aligned}$$

(A is a commutative R-algebra.) One can verify directly that $F_{m,R}$ is a subgroup scheme of $G_{m,R}$, under ordinary multiplication. Indeed, for

$u, v \in F_{m,R}(A)$,

$$\begin{aligned} uv &= \big(F_v(a) + \pi^j t\big)\big(F_v(b) + \pi^j s\big) \\ &= F_v(a)F_v(b) + \pi^j\big(sF_v(a) + tF_v(b) + \pi^j st\big) \\ &= F_v(a * b) + \pi^j\big(y + sF_v(a) + tF_v(b) + \pi^j st\big) \in F_{m,R}(A). \end{aligned}$$

Here $a * b$ is the group product in Spec $R[T_0, (1 + \pi^i T_0)^{-1}](A)$, and y is some element in A determined by (3.0). Moreover, we can define a group scheme homomorphism,

$$\Pi\colon F_{m,R} \to G_{m,R},$$

by $F_v(T_0) + \pi^j T_1 \mapsto (F_v(T_0) + \pi^j T_1)^p (1 + \pi^i T_0)^{-1}$. Observe that Spec $R[T_1, (1 + \pi^j T_1)^{-1}]$ and Spec $R[T_1, (1 + \pi^{pj})^{-1} T_1]$ are normal subgroup schemes of $F_{m,R}$ and $G_{m,R}$, respectively. We have

$$\begin{aligned} \Pi\big(1 + \pi^j T_1\big) = \Pi\big(F_v(0) + \pi^j T_1\big) &= \big(F_v(0) + \pi^j T_1\big)^p \big(1 + \pi^i \cdot 0\big)^{-1} \\ &= \big(1 + \pi^j T_1\big)^p, \end{aligned}$$

thus, Π restricted to Spec $R[T_1, (1 + \pi^j T_1)^{-1}]$ is the flat epimorphism,

$$\text{Spec } R\Big[T_1, \big(1 + \pi^j T_1\big)^{-1}\Big] \to \text{Spec } R\Big[T_1, \big(1 + \pi^{pj}\big)^{-1}\Big]$$

defined $T_1 \mapsto [(1 + \pi^j T_1)^p - 1]/\pi^{pj}$, see [4, Lemma I.1.2]. Thus Π induces a morphism of quotients,

$$\rho\colon \frac{F_{m,R}}{\text{Spec } R\Big[T_1, \big(1 + \pi^j T_1\big)^{-1}\Big]} \to \frac{G_{m,R}}{\text{Spec } R\Big[T_1, \big(1 + \pi^{pj} T_1\big)^{-1}\Big]}.$$

We identify these quotients with the group schemes F_{m,R_j} and $G_{m,R_{pj}}$ defined

$$F_{m,R_j}(A) = F_{m,R}\frac{A}{(\pi^j A)} \quad \text{and} \quad G_{m,R_{pj}}(A) = U\frac{A}{(\pi^{pj} A)},$$

see [11, Section 2, (8)]. Note

$$\begin{aligned} F_{m,R_j}(A) = \Big\{ u \in U(A) \,|\, & u = F_v(a) \\ & \text{for some } a \in \text{Spec } R\Big[T_0, \big(1 + \pi^i T_0\big)^{-1}\Big](A)\Big\}. \end{aligned}$$

In fact, ρ is now identified with the map,

$$\bar{\rho}\colon F_{m,R_j} \to G_{m,R_{pj}}$$

defined

$$\bar{\rho}\big(F_v(T_0)\big) = M\big(F_v(T_0)^p\big),$$

where M is the device defined in Section 3.

We have the following commutative diagram,

$$\begin{array}{ccc} F_{m,R} & \xrightarrow{s} & F_{m,R_j} \\ \Pi \downarrow & & \downarrow \bar{\rho}\ . \\ G_{m,R} & \xrightarrow{t} & G_{m,R_{pj}} \end{array}$$

Here s and t are the canonical surjections. Now with $F_v(T_0) + \pi^j T_1 \in F_{m,r}$, we have

$$(t \circ \Pi)\big(F_v(T_0) + \pi^j T_1\big) = (\bar{\rho} \circ s)\big(F_v(T_0) + \pi^j T_1\big),$$

hence

$$F_v(T_0)^p\big(1 + \pi^i T_0\big)^{-1} \equiv \bar{\rho}\big(F_v(T_0)\big) \pmod{\pi^{pj}},$$

which yields

$$\big(F_v(T_0) + \pi^j T_1\big)^p\big(1 + \pi^i T_0\big)^{-1} \equiv \bar{\rho}\big(F_v(T_0)\big) \pmod{\pi^{pj}},$$

or

$$\big(F_v(T_0) + \pi^j T_1\big)^p\big(1 + \pi^i T_0\big)^{-1} \equiv M\big(F_v(T_0)^p\big) \pmod{\pi^{pj}},$$

or

$$\big(F_v(T_0) + \pi^j T_1\big)^p\big(1 + \pi^i T_0\big)^{-1} \equiv G_v\big(\Theta_0(T_0)\big) \pmod{\pi^{pj}},$$

because $G_v(\Theta_0(T_0)) = M(F_v(T_0)^p)$. Thus Θ_1 has coefficients in R and Θ is a flat epimorphism. Moreover, $B/\langle\Theta\rangle \cong H_v(i,j)$, thus $\operatorname{Spec} H_v(i,j) \to \operatorname{Spec} B \xrightarrow{\Theta} \operatorname{Spec} C$ is an explicit flat resolution of $\operatorname{Spec} H_v(i,j)$ with $B = R[T_0, T_1, (1 + \pi^i T_0)^{-1}, (F_v(T_0) + \pi^j T_1)^{-1}]$ and $C = R[T_0, T_1, (1 + \pi^{pi} T_0)^{-1}, (G_v(T_0) + \pi^{pj} T_1)^{-1}]$.

4. CONSTRUCTION OF THE FORMAL GROUPS

In this section we compute polynomial formal groups from the flat short exact sequence constructed in Section 3. For this section, let $H_v(i,j)$ be a Greither order under the conditions $i' + j > \nu(1-v) \geq i' + (j/2)$ and $i + j \leq e/[p(p-1)]$. From Section 3 we have the flat resolution,

$$\operatorname{Spec} H_v(i,j) \to \operatorname{Spec} B \xrightarrow{\Theta} \operatorname{Spec} C,$$

with

$$B = R\Big[T_0, T_1, \big(1 + \pi^i T_0\big)^{-1}, \big(F_v(T_0) + \pi^j T_1\big)^{-1}\Big],$$

$$C = R\Big[T_0, T_1, \big(1 + \pi^{pi} T_0\big)^{-1}, \big(G_v(T_0) + \pi^{pj} T_1\big)^{-1}\Big],$$

and $H_v(i,j) \cong B/\langle \Theta_0(T_0), \Theta_1(T_0,T_1)\rangle$.

We now complete the R-Hopf algebra B at the augmentation ideal (the ideal generated by T_0 and T_1) to obtain the formal R-Hopf algebra $R[[T]]$, $T = (T_0, T_1)$, because

$$\frac{1}{1 + \pi^i T_0} \in R[[T_0]] \subseteq R[[T]],$$

and

$$\frac{1}{F_v(T_0) + \pi^j T_1} = \frac{1}{F_v(T_0)} \cdot \frac{1}{1 + F_v(T_0)^{-1} \pi^j T_1} \in R[[T_0]][[T_1]] = R[[T]].$$

We have

$$T_1 = \frac{\big(F_v(T_0) + \pi^j T_1\big) - F_v(T_0)}{\pi^j} = \frac{\big(F_v(T_0) + \pi^j T_1\big) - 1}{\pi^j} + \frac{1 - F_v(T_0)}{\pi^j}.$$

Now let $f(T_0)$ be the *formal Maclaurin series* expansion of $\pi^{-j}(1 - F_v(T_0))$. Because $F_v(0) = 1$, $f(T_0)$ can be written $\lambda^{-1} T_0 \cdot h(T_0)$ for some polynomial $h(T_0)$, with $\lambda = \pi^{j-i}((\zeta_1 - 1)/(1-v))$. Thus,

$$T_1 = \frac{\big(F_v(T_0) + \pi^j T_1\big) - 1}{\pi^j} + \lambda^{-1} T_0 \cdot h(T_0).$$

Now put $q(T_0) = \lambda^{-1}T_0(1 - h(T_0))$. Then the change of variables,

$$X_1 = T_0 \quad \text{and} \quad X_2 = T_1 + q(T_0)$$

yields the formal Hopf algebra $R[[X]]$, $X = (X_1, X_2)$, which equals $R[[T]]$. (If such a change of variables was not possible, then the quotient $B/\langle\Theta\rangle \cong H_v(i, j)$ could not be isomorphic to the R-Hopf order $R[\pi^{-i}(g^p - 1), \pi^{-j}(g - 1) + \lambda^{-1}\pi^{-i}(g^p - 1)]$ in Lemma 2.2.) Moreover, the comultiplication of $R[[X]]$ is given by polynomials, thus $R[X_1, X_2] = R[T_0, T_1]$ is a subbialgebra of $R[[X]]$. Now via the identification $R[X_1, X_2] \otimes R[X_1, X_2] \cong R[x_1, x_2, y_1, y_2]$, the polynomials $\Delta(X_1)$ and $\Delta(X_2)$ yield the polynomial formal group $\mathscr{F}$ given in Section 2 as (2.4), cf. [2, Appendix 2]. Observe that $R[X_1, X_2]_{\mathscr{F}} = R[T_0, T_1] \subseteq B$.

In this same sense, the completion of C at its augmentation ideal will give rise to another polynomial formal group $\mathscr{G}$ with $C \supseteq R[T_0, T_1] = R[X_1, X_2]_{\mathscr{G}}$. First, define a map $\Gamma(T_0, T_1) = (\Gamma_0(T_0), \Gamma_1(T_0, T_1))$ on Spec C by

$$\Gamma_0(T_0) = \frac{\left(1 + \pi^{pi}T_0\right)^p - 1}{\pi^{p^2 i}},$$

$$\Gamma_1(T_0, T_1) = \frac{\left(1 + \pi^{pi}T_0\right)^{-1}\left(G_v(T_0) + \pi^{pj}T_1\right)^p - J_v(\Gamma_0(T_0))}{\pi^{p^2 j}},$$

with $J_v(T_0) = N(M(G_v(T_0)^p))$. Here M, N are the devices defined in Section 3. Of course in this case M acts on polynomials of the form,

$$\alpha(T_0) = \sum_{m=0}^{kp} a_m\left(1 + \pi^{pi}T_0\right)^m, \qquad a_m \in K,$$

and is defined

$$\begin{aligned} M(\alpha(T_0)) &= (a_0 + a_1 + a_2 + \cdots + a_{p-1}) + (a_p + \cdots + a_{2p-1})\left(1 + \pi^{pi}T_0\right)^p \\ &\quad + (a_{2p} + \cdots + a_{3p-1})\left(1 + \pi^{pi}T_0\right)^{2p} + \cdots \\ &\quad + (a_{(k-1)p} + \cdots + a_{kp-1})\left(1 + \pi^{pi}T_0\right)^{(k-1)_p} \\ &\quad + a_{kp}\left(1 + \pi^{pi}T_0\right)^{kp}. \end{aligned}$$

Then $N(M(\alpha(T_0)))$ is that polynomial $\beta(T_0)$ so that $\beta(\Gamma(T_0)) = M(\alpha(T_0))$. In fact, with this polynomial $J_v(T_0)$, the R-algebra,

$$D = R\left[T_0, \left(1 + \pi^{p^2 i} T_0\right)^{-1}, T_1, \left(J_v(T_0) + \pi^{p^2 j} T_1\right)^{-1}\right]$$

is an R-Hopf algebra. Specifically, we have J_v satisfying

$$J_v(0) = 1 \quad \text{and} \quad J_v(X)J_v(Y) \equiv J_v(X + Y + \pi^{p^2 i} XY) \pmod{\pi^{p^2 j}}.$$

Our goal is to show that Γ: Spec $C \to$ Spec D is a flat map. This implies that the quotient $C/\langle \Gamma_0(T_0), \Gamma_1(T_0, T_1)\rangle$ is isomorphic to an R-Hopf order in KC_{p^2}. We then show that the comultiplication of this R-Hopf order is dictated by a polynomial formal group. We have the following theorem.

THEOREM 4.0. *Suppose* $i' + j > v(1 - v) \geq i' + (j/2)$ *and* $i + j \leq e/[p(p - 1)]$. *Then* Γ *is a flat map and the quotient* $C/\langle \Gamma_0(T_0), \Gamma_1(T_0, T_1)\rangle$ *is isomorphic to a Greither order* $H_w(pi, pj) \subseteq KC_{p^2}$, *with* $w = 1 - [(1 - v)^p]/[(\zeta_1 - 1)^{p-1}]$.

Proof. We first show that with $w = 1 - [(1 - v)^p]/[(\zeta_1 - 1)^{p-1}]$, there exists a Greither order $H_w(pi, pj)$. We have that $pj \leq i$ implies $p^2 j \leq pi$, with $0 \leq pj, pi \leq e/(p - 1)$. Moreover,

$$\begin{aligned} v(1 - w) &= v\left(\frac{(1 - v)^p}{(\zeta_1 - 1)^{p-1}}\right) \\ &= pv(1 - v) - e \\ &\geq pi' + \frac{pj}{2} - e \\ &= (pi)' + \frac{pj}{2} \\ &\geq (pi)' + j, \end{aligned}$$

with

$$\frac{e}{p(p - 1)} \geq i + j,$$

or

$$\frac{e}{p} \geq (p - 1)i + (p - 1)j,$$

or

$$\frac{e}{p - 1} - pi + j \geq \frac{e}{p(p - 1)} - i + pj,$$

or

$$(pi)' + j \geq \frac{1}{p}(pi)' + pj.$$

Hence $w \in U_{(pi)'+j} = U_{(pi)'+j} \cap U_{((pi)'/p)+pj}$, which says that the R-Hopf order $H_w(pi, pj)$ exists, confer [4, Corollary I.3.6].

Now consider the R-algebra,

$$S = R\left[\frac{g^p - 1}{\pi^{pi}}, \frac{g - b}{\pi^{pj}}\right] \subseteq KC_{p^2}, \qquad \langle g \rangle = C_{p^2},$$

where $b = G_v((g^p - 1)/\pi^{pi})$. If S is an R-Hopf order in KC_{p^2}, then Γ is a flat map, and the quotient $C/\langle\Gamma\rangle$ is a finite R-Hopf algebra isomorphic to S. (This follows because $\Gamma_0(T_0) = 0$ and $\Gamma_1(T_0, T_1) = 0$ imply that $1 + \pi^{pi}T_0 \in C$ and $G_v(T_0) + \pi^{pj}T_1 \in C$ correspond to elements g^p and g in S, respectively.)

We claim that S is an R-Hopf order in KC_{p^2} isomorphic to the Greither order $H_w(pi, pj)$. Let

$$\left(1, G_v\left(\frac{\zeta_1 - 1}{\pi^{pi}}\right), G_v\left(\frac{\zeta_1^2 - 1}{\pi^{pi}}\right), \ldots, G_v\left(\frac{\zeta_1^{p-1} - 1}{\pi^{pi}}\right)\right)$$

be the image of b in the maximal integral order R^p under the embedding $g^p \mapsto (1, \zeta_1, \zeta_1^2, \ldots, \zeta_1^{p-1})$, and let $y = G_v((\zeta_1 - 1)/\pi^{pi})$. The R-algebra S is an R-Hopf order isomorphic to $H_w(pi, pj)$ if and only if $v(y - w) \geq (pi)' + pj$ by [4, Corollary I.3.6].

We first consider the case $p = 2$. Then

$$F_v(T_0) = \frac{1 + v}{2} + \frac{1 - v}{2}(1 + \pi^i T_0),$$

thus

$$\begin{aligned} G_v(T_0) &= N\left(M\left(F_v(T_0)^2\right)\right) \\ &= N\left(\left(\frac{1 + v}{2}\right)^2 + \left(\frac{1 - v^2}{2}\right) + \left(\frac{1 - v}{2}\right)^2 (1 + \pi^i T_0)^2\right) \\ &= \left(\frac{1 + v}{2}\right)^2 + \left(\frac{1 - v^2}{2}\right) + \left(\frac{1 - v}{2}\right)^2 (1 + \pi^{2i} T_0). \end{aligned}$$

Hence,

$$b = \left(\frac{1+v}{2}\right)^2 + \left(\frac{1-v^2}{2}\right) + \left(\frac{1-v}{2}\right)^2 g^2, \qquad \langle g \rangle = C_4,$$

with

$$\begin{aligned} y &= G_v\left(\frac{\zeta_1 - 1}{\pi^{2i}}\right) \\ &= \left(\frac{1+v}{2}\right)^2 + \left(\frac{1-v^2}{2}\right) - \left(\frac{1-v}{2}\right)^2 \\ &= 1 - \frac{(1-v)^2}{-2} = w. \end{aligned}$$

It follows that $\nu(y-w) = \nu(0) > (2i)' + 2j$, therefore $S \cong H_w(2i, 2j)$ as R-Hopf orders in KC_4 by [4, Corollary I.3.6].

Next we consider the case $p > 2$. By the definition of $G_v(T_0)$, with $\zeta = \zeta_1$,

$$y = G_v\left(\frac{\zeta - 1}{\pi^{pi}}\right) = E_0^p + E_1^p\zeta + \cdots + E_{p-1}^p\zeta^{p-1} + \sum_\iota pr_\iota E_0^{i_0}E_1^{i_1}\cdots E_{p-1}^{i_{p-1}},$$

where the sum is taken over all partitions $\iota = (i_0, \ldots, i_{p-1})$, $i_0 + \cdots + i_{p-1} = p$, $0 \le i_k < p$. Here the r_ι are elements of R dependent on the partition ι, and the E_k, $0 \le k \le p-1$ are defined

$$E_k = \frac{1}{p}\sum_{m=0}^{p-1} \zeta^{-km} v^m.$$

We first show that $\nu(y - \sum_{k=0}^{p-1} E_k^p \zeta^k) \ge (pi)' + pj$. We claim the sum,

$$\sum_\iota pr_\iota E_0^{i_0}E_1^{i_1}\cdots E_{p-1}^{i_{p-1}}$$

has value at least $\nu([(1-v^p)^{p-1}]/p^{p-1})$. To see this note

$$\nu\left(pr_\iota E_0^{i_0}E_1^{i_1}\cdots E_{p-1}^{i_{p-1}}\right) = \nu\left(\frac{pr_\iota(1-v^p)^p}{p^p(1-v)^p}\right),$$

because $E_k = (1 - \upsilon^p)/[p(1 - \zeta^{-k}\upsilon)]$ for $0 \le k \le p - 1$, and $\nu(1 - \zeta^{-k}) > \nu(1 - \upsilon)$. Moreover,

$$\nu\left(\frac{pr_\iota(1 - \upsilon^p)^p}{p^p(1 - \upsilon)^p}\right) = \nu\left(\frac{r_\iota(1 - \upsilon^p)^p}{p^{p-1}(1 - \upsilon)^p}\right)$$
$$\ge \nu\left(\frac{(1 - \upsilon^p)^{p-1}}{p^{p-1}}\right),$$

because $\nu((1 - \upsilon)^p) = \nu(1 - \upsilon^p)$.

Now,

$$\nu\left(\sum_\iota pr_\iota E_0^{i_0}E_1^{i_1} \cdots E_{p-1}^{i_{p-1}}\right) \ge \nu\left(\frac{(1 - \upsilon^p)^{p-1}}{p^{p-1}}\right)$$
$$= (p - 1)\frac{pi' + pj}{2} - (p - 1)e$$
$$= (p - 1)\left(\frac{pe}{p - 1} - pi + \frac{pj}{2}\right) - (p - 1)e$$
$$= pe - (p - 1)pi + \frac{(p - 1)pj}{2} - (p - 1)e$$
$$= e - (p - 1)pi + \frac{(p - 1)pj}{2}.$$

In addition, $p > 2$ and $e/[p(p - 1)] \ge i + j$ imply

$$\frac{e}{p(p - 1)} \ge i - \frac{j(p - 3)}{2(p - 2)},$$

or

$$\frac{(p - 2)e}{p(p - 1)} \ge (p - 2)i - \frac{j(p - 3)}{2},$$

or

$$\frac{e(p - 2)}{p - 1} \ge p(p - 2)i + \frac{pj(3 - p)}{2},$$

or

$$\frac{e(p-1)}{p-1} - \frac{e}{p-1} \geq pi(p-1-1) + pj\left(1 - \frac{p-1}{2}\right),$$

or

$$e - \frac{e}{p-1} \geq (p-1)pi - pi + pj - \frac{(p-1)pj}{2},$$

or

$$e - (p-1)pi + \frac{(p-1)pj}{2} \geq \frac{e}{p-1} - pi + pj,$$

or

$$e - (p-1)pi + \frac{(p-1)pj}{2} \geq (pi)' + pj.$$

Thus,

$$\nu\left(\sum_{\iota} pr_{\iota} E_0^{i_0} E_1^{i_1} \cdots E_{p-1}^{i_{p-1}}\right) \geq (pi)' + pj,$$

and we conclude that $\nu(y - \sum_{k=0}^{p-1} E_k^p \zeta^k) \geq (pi)' + pj$.

We next show that $\nu((\sum_{k=0}^{p-1} E_k^p \zeta^k) - w) \geq (pi)' + pj$. Let $c = (c_0, c_1, \ldots, c_{p(p-1)})$ be the $(p(p-1)+1)$-tuple of coefficients with

$$\sum_{i=0}^{p(p-1)} c_i X^i = (1 + X + X^2 + \cdots + X^{p-1})^p,$$

X indeterminate. We have

$$\begin{aligned}
&\sum_{k=0}^{p-1} E_k^p \zeta^k \\
&\quad = E_0^p + E_1^p \zeta + \cdots + E_{p-1}^p \zeta^{p-1} \\
&\quad = \left(\frac{1}{p} \sum_{m=0}^{p-1} v^m\right)^p + \left(\frac{1}{p} \sum_{m=0}^{p-1} \zeta^{-m} v^m\right)^p \zeta + \cdots \\
&\qquad + \left(\frac{1}{p} \sum_{m=0}^{p-1} \zeta^{-(p-1)m} v^m\right)^p \zeta^{p-1} \\
&\quad = \frac{1}{p^p}\left(pc_1 v + pc_{p+1} v^{p+1} + pc_{2p+1} v^{2p+1} + \cdots + pc_{p(p-2)+1} v^{p(p-2)+1}\right).
\end{aligned}$$

Now consider the *formal Taylor series* expansion of

$$f(v) = \frac{1}{p^p}\Big(pc_1 v + pc_{p+1}v^{p+1} + pc_{2_p+1}v^{2^p+1} + \cdots + pc_{p(p-2)+1}v^{p(p-2)+1}\Big) - w,$$

as a function of v about the point 1. Recall $w = 1 - [(1-v)^p]/[(\zeta - 1)^{p-1}]$. We have

$$f(v) = \sum_{k=0}^{p(p-2)+1} A_k (v-1)^k,$$

with $A_k = (f^{[k]}(1))/k!$. Here $f^{[k]}(v)$ is the kth formal derivative of $f(v)$. We claim that $\nu(f(v)) \geq \nu(1-v)$. To this end, let $0 \leq k < p$, and consider the term $(f^{[k]}(1))/k!(v-1)^k$. By a direct calculation we have $f^{[0]}(1) = f(1) = 0$, thus the first term in the Taylor series is 0. Now for $1 \leq k < p$, a computation shows that $\nu(f^{[k]}(1)) \geq 0$, with $\nu(k!) = 0$. Hence the terms indexed by k, $0 \leq k < p$ have value at least $\nu(1-v)$. Moreover, let $p < k \leq p(p-2)+1$. The corresponding terms in the Taylor series can be written

$$\frac{f^{[k]}(1)(v-1)^{k-1}(v-1)}{k!}.$$

Observe that because $\nu(f^{[k]}(1)) \geq 0$, $k - 1 \geq p$, and $\nu(k!) = e$,

$$\nu\left(\frac{(v-1)^{k-1}}{k!}\right) \geq \nu\left(\frac{(v-1)^p}{p}\right) = \nu(1-w) \geq 0.$$

Thus $f^{[k]}(1)[(v-1)^{k-1}]/k!$ is in R, and we conclude that the terms indexed by k, $p < k \leq p(p-2)+1$ have value at least $\nu(1-v)$.

Lastly, we consider the term with $k = p$. In this case,

$$\nu\left(\frac{f^{[p]}(1)(v-1)^p}{p!}\right) \geq \nu\left(\frac{(\zeta-1)(1-v)^p}{p!}\right) \geq \nu\left(\frac{(1-v)^p}{p!}(1-v)\right),$$

because $\nu(f^{[p]}(1)) \geq \nu(\zeta - 1) > \nu(1 - v)$. It follows that $f(v) = (\sum_{k=0}^{p-1} E_k^p \zeta^k) - w$ has a value at least $\nu(1 - v)$. Now because

$$\begin{aligned}\nu(1 - v) &\geq i' + \frac{j}{2} = \frac{e}{p-1} - i + \frac{j}{2} \\ &\geq \frac{e}{p-1} - (p-1)i \\ &\geq \frac{e}{p-1} - pi + pj \\ &\geq (pi)' + pj,\end{aligned}$$

we conclude $\nu(y - w) \geq (pi)' + pj$ and $S \cong H_w(pi, pj)$. This completes the proof of Theorem 4.0. ∎

We now obtain a polynomial formal group which determines the comultiplication of the R-Hopf order $H_w(pi, pj)$. The generator $(g - a_w)/\pi^{pj}$ of $H_w(pi, pj) \cong C/\langle\Gamma\rangle$ can be decomposed in the same way the generator $(g - a_v)/\pi^j$ of $H_v(i, j)$ was decomposed in Section 2. We have

$$\begin{aligned}\frac{g - a_w}{\pi^{pj}} &= \frac{g-1}{\pi^{pj}} + \frac{1 - a_w}{\pi^{pj}} \\ &= \frac{g-1}{\pi^{pj}} + \frac{1}{\pi^{pj}}\left((1-w)f_1 + (1-w^2)f_2 + \cdots + (1-w^{p-1})f_{p-1}\right) \\ &= \frac{g-1}{\pi^{pj}} + \frac{(1-w)(g^p - 1)}{(\zeta_1 - 1)\pi^{pj}}\Omega_w.\end{aligned}$$

Here ζ_1 is a primitive pth root of unity, the f_i are idempotents for the maximal integral order in KC_p, and

$$\begin{aligned}\Omega_w = f_1 + \left(\frac{\zeta_1 - 1}{\zeta_1^2 - 1}\right)(1 + w)f_2 + \cdots + \left(\frac{\zeta_1 - 1}{\zeta_1^{p-1} - 1}\right) \\ \times (1 + w + \cdots + w^{p-2})f_{p-1}.\end{aligned}$$

LEMMA 4.1. *Under the conditions* $i + j \leq e/[p(p-1)]$, $i' + j > \nu(1 - v) \geq i' + (j/2)$, *and* $pj \leq i$, *the Greither order* $H_w(pi, pj)$ *can be written*

$$R\left[\frac{g^p - 1}{\pi^{pi}}, \frac{g-1}{\pi^{pj}} + \frac{g^p - 1}{\tau\pi^{pi}}\right],$$

where $\tau = \pi^{pj-pi}((\zeta_1 - 1)/(1 - w))$.

Proof. This follows as in Lemma 2.2 because $\nu(1-v) \geq i' + (j/2)$ implies

$$\begin{aligned}\nu(1-w) &= p\nu(1-v) - e \\ &\geq pi' + \frac{pj}{2} - e \\ &= (pi)' + \frac{pj}{2}.\end{aligned}$$

The condition $\nu(1-w) \geq (pi)' + (pj/2)$ is precisely the condition for which

$$\frac{(1-w)(g^p-1)}{(\zeta_1-1)\pi^{pj}}\Omega_w - \frac{(1-w)(g^p-1)}{(\zeta_1-1)\pi^{pj}} \in R\left[\frac{g^p-1}{\pi^{pi}}\right],$$

via [4, Theorem I.3.2a]. ∎

THEOREM 4.2. *Suppose* $i + j \leq e/[p(p-1)]$, $pj \leq i$, *and* $i' + j > \nu(1-v) \geq i' + (j/2)$. *Then the class* $[w] \in U_{(pi)'+j}/U_{(pi)'+pj}$, *with* $w = 1 - [(1-v)^p]/[(\zeta-1)^{p-1}]$, *corresponds to a Greither order*,

$$H_w(pi, pj) = R\left[\frac{g^p-1}{\pi^{pi}}, \frac{g-a_w}{\pi^{pj}}\right].$$

Moreover, there exists a polynomial formal group of the form,

$$\begin{aligned}\mathcal{G}(\bar{x}, \bar{y}) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} \pi^{pi} & 0 \\ \dfrac{\pi^{pi}\tau + \pi^{pj}}{\tau^2} & \dfrac{-\pi^{pj}}{\tau} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_1 \\ + \begin{pmatrix} 0 & 0 \\ \dfrac{-\pi^{pj}}{\tau} & \pi^{pj} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_2, \qquad (4.3)\end{aligned}$$

where $\tau = \pi^{pj-pi}((\zeta_1 - 1)/(1-w))$, *which determines the comultiplication of* $H_w(pi, pj)$.

Proof. This follows as in the proof of Theorem 2.3. We note that

$$\begin{aligned}\lambda^p &= \left(\pi^{j-i}\left(\frac{\zeta_1 - 1}{1 - \upsilon}\right)\right)^p \\ &= \frac{\pi^{pj-pi}(\zeta_1 - 1)^p}{(1 - \upsilon)^p} \\ &= \frac{\pi^{pj-pi}(\zeta_1 - 1)^p}{(\zeta_1 - 1)^{p-1}(1 - w)} \\ &= \tau.\end{aligned}$$

∎

We now complete the R-Hopf algebra $C = R[T_0, T_1, (1 + \pi^{pi}T_0)^{-1}, (G_\upsilon(T_0) + \pi^{pj}T_1)^{-1}]$ at the augmentation ideal to obtain the formal Hopf algebra $R[[T]]$, which under a suitable change of variables, is equal to the formal Hopf algebra $R[[X]]$. In this case, the comultiplication of $R[[X]]$ yields the polynomial formal group $\mathcal{G}(\bar{x}, \bar{y})$. We have $C \supseteq R[T_0, T_1] = R[X_1, X_2]_{\mathcal{G}}$.

5. PROOF OF THE MAIN THEOREM

THEOREM 5.0 (Main Theorem). *Let $H = H_\upsilon(i, j)$ be a Greither order in KC_{p^2} with $i + j \le e/[p(p - 1)]$, $pj \le i$, and $\nu(1 - \upsilon) \ge i' + (j/2)$. Then $H_\upsilon(i, j)$ represents the kernel of an isogeny of polynomial formal groups.*

Proof. Case I. $\nu(1 - \upsilon) \ge i' + j$. In this case $H_\upsilon(i, j)$ is the Larson order $H(i, j)$. By [15, Theorem 2.0], we have the flat short exact sequence of group schemes,

$$\operatorname{Spec} H(i, j) \to \operatorname{Spec} B \xrightarrow{\Theta} \operatorname{Spec} C,$$

with R-Hopf algebras,

$$B = R\left[T_0, \left(1 + \pi^i T_0\right)^{-1}, T_1, \left(1 + \pi^j T_1\right)^{-1}\right],$$

$$C = R\left[T_0, \left(1 + \pi^{pi} T_0\right)^{-1}, T_1, \left(1 + \pi^{pj} T_1\right)^{-1}\right],$$

(T_0, T_1 indeterminate.) The flat epimorphism Θ is defined $\Theta(T_0, T_1) = \Theta(\Theta_0(T_0), \Theta_1(T_0, T_1))$ with

$$\Theta_0(T_0) = \frac{\left(1 + \pi^i T_0\right)^p - 1}{\pi^{pi}},$$

$$\Theta_1(T_0, T_1) = \frac{\left(1 + \pi^i T_0\right)^{-1}\left(1 + \pi^j T_1\right)^p - 1}{\pi^{pj}}.$$

Moreover, one checks that the variation Θ' of Θ defined $\Theta'(T_0, T_1) = \Theta'(\Theta_0(T_0), \Theta_1'(T_0, T_1))$ with

$$\Theta_1'(T_0, T_1) = \frac{\left(1 + \pi^i T_0\right)^{p-1}\left(1 + \pi^j T_1\right)^p - 1}{\pi^{pj}},$$

also serves as a flat epimorphism Θ': Spec $B \to$ Spec C. Because Θ' is a homomorphism of group schemes we have

$$\Theta'(U *_B V) = \Theta'(U) *_C \Theta'(V), \tag{5.1}$$

where $U, V \in$ Spec B, $*_B$ is the multiplication in Spec B, and $*_C$ is multiplication in Spec C.

Now the completion of B at the augmentation ideal yields the formal Hopf algebra $R[[T]]$ and the polynomial formal group (2.1),

$$\mathscr{F}(\bar{x}, \bar{y}) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} \pi^i & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_1 + \begin{pmatrix} 0 & 0 \\ 0 & \pi^j \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_2.$$

We have $B \supseteq R[T_0, T_1] = R[X_1, X_2]_{\mathscr{F}}$. Likewise, the completion of C at its augmentation ideal yields the polynomial formal group,

$$\mathscr{G}(\bar{x}, \bar{y}) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} \pi^{pi} & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_1 + \begin{pmatrix} 0 & 0 \\ 0 & \pi^{pj} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_2.$$

(One shows directly that $\mathscr{G}$ is a formal group via Section 1.) We have $C \supseteq R[T_0, T_1] = R[X_1, X_2]_{\mathscr{G}}$.

Now let $\Psi(\bar{x})$ be the 2-tuple of polynomials $\Psi(\bar{x}) = (\Psi_1(\bar{x}), \Psi_2(\bar{x}))$ defined

$$\Psi_1(\bar{x}) = \frac{\left(1 + \pi^i x_1\right)^p - 1}{\pi^{pi}},$$

$$\Psi_2(\bar{x}) = \frac{\left(1 + \pi^i x_1\right)^{p-1}\left(1 + \pi^j x_2\right)^p - 1}{\pi^{pj}}.$$

Then the homomorphism condition (5.1) translates to the condition,

$$\Psi_i(\mathscr{F}(\bar{x}, \bar{y})) = \mathscr{G}_i(\Psi(\bar{x}), \Psi(\bar{y})),$$

for $i = 1, 2$. Thus Ψ: $\mathscr{F} \to \mathscr{G}$ is a homomorphism of polynomial formal groups. Now because

$$\frac{R[X_1, X_2]_{\mathscr{F}}}{\langle \Psi_1(X), \Psi_2(X) \rangle} \cong H(i, j),$$

Ψ is an isogeny of polynomial formal groups whose kernel is represented by $H(i, j)$. This completes the proof of Case I.

Case II. $i' + j > \nu(1 - \upsilon)$. In this case $H_\upsilon(i, j)$ is a non-Larson R-Hopf order in KC_{p^2}. We begin by recalling the flat short exact sequence of group schemes,

$$Sp H_\upsilon(i, j) \to \operatorname{Spec} B \xrightarrow{\Theta} \operatorname{Spec} C,$$

with R-Hopf algebras,

$$B = R\Big[T_0, \big(1 + \pi^i T_0\big)^{-1}, T_1, \big(F_\upsilon(T_0) + \pi^j T_1\big)^{-1}\Big],$$

$$C = R\Big[T_0, \big(1 + \pi^{pi} T_0\big)^{-1}, T_1, \big(G_\upsilon(T_0) + \pi^{pj} T_1\big)^{-1}\Big].$$

Here

$$F_\upsilon(T_0) = \frac{1}{p} \sum_{m=0}^{p-1} \upsilon^m \sum_{n=0}^{p-1} \zeta_1^{-mn} \big(1 + \pi^i T_0\big)^n,$$

and $G_\upsilon(T_0)$ is the polynomial $N(M(F_\upsilon(T_0)^p))$ constructed in Section 3. Θ is defined $\Theta(T_0, T_1) = \Theta(\Theta_0(T_0), \Theta_1(T_0, T_1))$ with

$$\Theta_0(T_0) = \frac{\big(1 + \pi^i T_0\big)^p - 1}{\pi^{pi}},$$

$$\Theta_1(T_0, T_1) = \frac{\big(1 + \pi^i T_0\big)^{-1} \big(F_\upsilon(T_0) + \pi^j T_1\big)^p - G_\upsilon(\Theta_0(T_0))}{\pi^{pj}}.$$

Moreover, Θ' given $\Theta'(T_0, T_1) = \Theta'(\Theta_0(T_0), \Theta_1'(T_0, T_1))$ with

$$\Theta_1'(T_0, T_1) = \frac{\big(1 + \pi^i T_0\big)^{p-1} \big(F_\upsilon(T_0) + \pi^j T_1\big)^p - G_\upsilon(\Theta_0(T_0))}{\pi^{pj}}$$

is also a flat epimorphism Spec $B \to$ Spec C. Note that Θ' is a homomorphism of group schemes Θ': Spec $B \to$ Spec C, i.e.,

$$\Theta'(U *_B V) = \Theta'(U) *_C \Theta'(V), \tag{5.2}$$

where $U, V \in$ Spec B, $*_B$ is the multiplication in Spec B, and $*_C$ is multiplication in Spec C.

Now the completion of B at the augmentation ideal yields the formal Hopf algebra $R[[T]] = R[[X]]$ (under the change of variables $X_1 = T_0$,

$X_2 = T_1 + q(T_0)$), and the polynomial formal group (2.4),

$$\mathscr{F}(\bar{x}, \bar{y}) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} \pi^i & 0 \\ \dfrac{\pi^i\lambda + \pi^j}{\lambda^2} & \dfrac{-\pi^j}{\lambda} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_1 + \begin{pmatrix} 0 & 0 \\ \dfrac{-\pi^j}{\lambda} & \pi^j \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_2.$$

We have that $B \supseteq R[T_0, T_1] = R[X_1, X_2]_{\mathscr{F}}$. Likewise, the completion of C at the augmentation ideal yields $R[[T]] = R[[X]]$, with the comultiplication of $R[[X]]$ defining the polynomial formal group (4.3),

$$\mathscr{G}(\bar{x}, \bar{y}) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} \pi^{pi} & 0 \\ \dfrac{\pi^{pi}\tau + \pi^{pj}}{\tau^2} & \dfrac{-\pi^{pj}}{\tau} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_1 + \begin{pmatrix} 0 & 0 \\ \dfrac{-\pi^{pj}}{\tau} & \pi^{pj} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} y_2.$$

Observe that $C \supseteq R[T_0, T_1] = R[X_1, X_2]_{\mathscr{G}}$.

Now let $\Psi(\bar{x}) = (\Psi_1(\bar{x}), \Psi_2(\bar{x}))$ be a 2-tuple of polynomials defined

$$\Psi_1(\bar{x}) = \frac{\left(1 + \pi^i x_1\right)^p - 1}{\pi^{pi}},$$

$$\Psi_2(\bar{x}) = \frac{\left(1 + \pi^i x_1\right)^{p-1}\left(F_v(x_1) + \pi^j\left(x_2 - q(x_1)\right)\right)^p - G_v(\Psi_1(\bar{x}))}{\pi^{pj}}.$$

Then the homomorphism condition (5.2) translates to the condition,

$$\Psi_i(\mathscr{F}(\bar{x}, \bar{y})) = \mathscr{G}_i(\Psi(\bar{x}), \Psi(\bar{y})),$$

for $i = 1, 2$. Thus $\Psi\colon \mathscr{F} \to \mathscr{G}$ is a homomorphism of polynomial formal groups. Now because

$$\frac{R[X_1, X_2]_{\mathscr{F}}}{\langle \Psi_1(X), \Psi_2(X) \rangle} \cong H_v(i, j),$$

Ψ is an isogeny of polynomial formal groups whose kernel is represented by $H_v(i, j)$. This completes the proof of the Main Theorem.

REFERENCES

1. L. N. Childs, D. J. Moss, J. Sauerberg, and K. Zimmermann, Dimension one polynomial formal groups, *in* ''Hopf Algebras, Polynomial Formal Groups and Raynaud Orders,'' monograph, Memoirs Am. Math. Soc., Vol. 136, p. 651, Am. Math. Soc., Providence, RI, 1998.
2. L. N. Childs, D.J. Moss, J. Sauerberg, and K. Zimmermann, Dimension two polynomial formal groups and Hopf algebras, *in* ''Hopf Algebras, Polynomial Formal Groups and Raynaud Orders,'' monograph, Memoirs Am. Math. Soc., Vol. 136, p. 651, Am. Math. Soc., Providence, RI, 1998.
3. L. N. Childs, C. Greither, D. J. Moss, J. Sauerberg, and K. Zimmermann, Introduction to polynomial formal groups and Hopf algebras, *in* ''Hopf Algebras, Polynomial Formal Groups and Raynaud Orders,'' monograph, Memoirs Am. Math. Soc., Vol. 136, p. 651, Am. Math. Soc., Providence, RI, 1998.
4. C. Greither, Extensions of finite groups schemes, and Hopf Galois theory over a complete discrete valuation ring, *Math. Z.* **210** (1992), 37–67.
5. R. Larson, Hopf algebra orders determined by group valuations, *J. Algebra* **38** (1976), 414–452.
6. J. S. Milne, ''Etale Cohomology,'' Princeton Univ. Press, Princeton, NJ, 1980.
7. J. S. Milne, ''Arithmetic Duality Theorems,'' Academic Press, Boston, 1986.
8. L. Roberts, The flat cohomology of group schemes of order p, *Amer. J. Math.* **95** (1973), 688–702.
9. T. Sekiguchi, On the deformations of Witt groups to tori, II, *J. Algebra* **138**(2) (1991), 273–297.
10. T. Sekiguchi and N. Suwa, Théories de Kummer–Artin–Schreier–Witt, *Comptes Rendus de l'Acad. des Sci.* **319**(I) (1994), 105–110.
11. T. Sekiguchi and N. Suwa, On the unified Kummer–Artin–Schreier–Witt theory, Chuo University Preprint Series, No. 41, Chuo University, Bunkyoku, Tokyo, Japan, 1994.
12. R. G. Underwood, Hopf algebra orders over a complete discrete valuation ring, their duals and extensions of R-groups, doctoral dissertation, State University of New York at Albany, 1992.
13. R. G. Underwood, R-Hopf algebra orders in KC_{p^2}, *J. Algebra* **169** (1994), 418–440.
14. R. G. Underwood, The valuative condition and R-Hopf algebra orders in KC_{p^3}, *Amer. J. Math.* **118**(4) (1996), 701–743.
15. R. G. Underwood, The group of Galois extensions over orders in KC_{p^2}, *Trans. Amer. Math. Soc.* **349** (1997), 1503–1514.